UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,556	06/13/2005	Bonnie C. Sexton	US02 0576 US	5050

65913 7590 08/13/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
08/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/538,556	SEXTON, BONNIE C.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-18* is/are rejected.

7)☐ Claim(s) *3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are pending.

2. Amendment After Final filed 08/06/2009 has been received and considered. Prosecution is hereby re-opened.

Priority

3. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 119(e) as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosure of the prior-filed application, Application No. 60433365, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. The provisional application fails to provide an enabling disclosure for claims 1-18 of the present invention as it merely contains ideas the applicant's intend to perform without any explanation how the ideas will be fulfilled. Specifically, each independent claim contains affine and inverse

affine transformations which are not even mentioned in Application No. 60433365 and each dependent claim that further limits the invention are additionally not described in 60433365. Therefore, claims 1-18 are not given the priority claimed in Application No. 60433365 to December 13, 2002.

The priority claims to Application No. 60473527 to May 27, 2003 is proper and the claims have been examined with respect to this date.

Claim Objections

4. The objection to claim 4 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 2, 4, 5, 8-10, 12-15 and 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Van Buer (US 20030198345).

As per claims 1, 4, 5, 12 and 14, Van Buer discloses an apparatus for encryption and decryption by performing a SubByte function of the Rijndael Block Cipher, comprising: an S-box constructed by composing a first and second transformation,

wherein the first transformation is a look-up table for the multiplicative inverse in the finite field GF(2^8), and performing a non-linear byte substitution using the composed S-Box (see paragraphs [0067]-[0069]) and the second transformation is, an affine-all transformation that performs both an affine and inverse affine transformation (see paragraphs [0067]-[0069] and [0083]-[0088]).

As per claims 2 and 18, Van Buer discloses the look-up table is the multiplicative inverse in the finite field GF(2^8) (see paragraph [0068]), the affine-all transformation is implemented using a combinational logic circuit (see Fig. 4), that in the look-up table has {00} mapped to itself (see Table 1 on page 6).

As per claim 8, Van Buer discloses a plurality of instances of a data processing module arranged in a data processing pipeline (see paragraph [0067]).

As per claim 9, Van Buer discloses the apparatus is arranged to perform encryption or decryption in accordance with the Rijndael Block Cipher, and wherein the data processing module is arranged to implement a Rijndael round (see paragraphs [0064] and [0069]).

As per claim 10,Van Buer discloses the data processing module is arranged to implement the SubByte transformation of the Rijndael round using the look-up table composed with the affine transformation for encryption and the inverse affine transformation for decryption (see paragraphs [0067]-[0069]).

As per claims 13 and 15, Van Buer discloses means for obtaining the multiplicative inverse is a look-up table and said means for performing the affine-all

transformation is a combinational logic circuit (paragraphs [0067]-[0069] and [0083]-[0089]).

Claim Rejections - 35 USC § 103

7. Claims 6, 7, 11, 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Buer as applied to claims 1, 4, 5, 10 and 14 above, in view of Dent (US 5091942).

As per claims 6, 7, 11, 16 and 17, Van Buer fails to explicitly disclose the look-up table is implemented in ROM.

However, Dent teaches the use of ROM for a look-up table (see column 26 lines 29-48).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the lookup table of Van Buer in ROM and for the circuit to implement the equations.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to allow the values of the table to be read but not changed.

Allowable Subject Matter

8. Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to teach the implementation of the specific equations as put for in claim 3 in combination with the remaining limitations.

Response to Arguments

10. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2137